Express Mail No.: EL485651147US

Date of Mailing: September 21, 2000

Atty Docket No. 00P7906US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

This is a U.S. NONPROVISIONAL Patent Application for:

Title: **PROCESSING ELECTRONIC MESSAGES**

Inventor: William J. Beyda
Address: 21580 Edward Way, Cupertino, California 95014
Citizenship: United States of America

PROCESSING ELECTRONIC MESSAGES

TECHNICAL FIELD

This invention relates to systems and methods for processing electronic messages.

BACKGROUND

Electronic messaging services, including electronic mail, voice mail and digital facsimile (or fax), are common in today's business and home environments. Electronic messaging is a powerful communications tool that enables users to exchange information and collaborate across great distances and disparate time zones. Electronic messaging systems typically allow users to exchange messages over a network, including a common local area network (LAN) and an external network (e.g., the Internet). Electronic messaging systems also typically allow users to save, copy, and forward received messages. Many electronic messaging systems provide universal or unified messaging services for handling arbitrarily complex multimedia objects. For example, the Xpressions™ unified messaging system (available from Siemens Information and Communication Networks, Inc. of Boca Raton, Florida, U.S.A.) provides unified messaging services for handling voice mail, fax, e-mail and other types of electronic media. The Xpressions™ system provides an all-in-one mailbox (or personal message) center that users may access with a computer or a telephone to manage their messages.

A wide variety of digital content types may be transmitted through today's electronic messaging systems. A substantial amount of digital content, however, is subject to certain access restriction conditions. For example, some digital content (e.g., copyrighted works, such as textual works, musical works and video works) may not be copied or transmitted without the authorization of the copyright owner. Other digital content (e.g., proprietary works, confidential works and for internal use only works) may be copied and transmitted, but only a limited number of people may be authorized to have access to that content.

SUMMARY

The invention features an electronic messaging scheme that is configurable to prevent intentional and unintentional transmission of electronic messages subject to one or more access restriction conditions.

In one aspect, the invention features an electronic messaging scheme in which an electronic message is interrogated for an access restriction notice in response to a user command to transmit the electronic message, and a detected access restriction notice is responded to in accordance with a prescribed transmission policy.

Embodiments of the invention may include one or more of the following features.

The electronic message may be interrogated by detecting an ownership notice (e.g., a copyright notice) in the electronic message. An ownership notice may be detected by comparing one or more characters in the electronic message to one or more stored ownership notice representations. An ownership notice may be detected by interrogating a header component of the electronic message.

Characters in an image component of the electronic message (e.g., a still image or a video image) may be translated into computer-readable character representations. An access restriction notice may be detected by comparing one or more translated computer-readable character representations to one or more stored access restriction representations.

A detected access restriction notice may be responded to in a variety of ways. For example, a detected access restriction may be responded to by blocking transmission of the electronic message in response to a detected access restriction notice. A detected access restriction notice may be responded to by enabling a user or a system administrator to override a blocked electronic message transmission. A detected access restriction notice may be responded to by displaying a report to a user in response to a detected access restriction notice. A detected access restriction notice may be responded to by displaying to a user a message reporting that the electronic message cannot be transmitted because of a detected access restriction. A detected access restriction notice may be responded to by displaying to a user a message reporting that a fee must be paid to enable transmission of the electronic message.

Among the advantages of the invention are the following.

The invention protects users and their employers from potential liability (e.g., liability to copyright owners for unauthorized reproduction or distribution of their copyrighted works) and potential loss of corporate assets (e.g., trade secret information) that otherwise could result from the intentional or unintentional distribution of certain kinds of electronic messages.

Other features and advantages of the invention will become apparent from the following description, including the drawings and the claims.

DESCRIPTION OF DRAWINGS

FIG. 1 is a block diagram of a universal messaging system, including a universal message server, a communications server and a plurality of communications terminals.

FIG. 2 is a block diagram of the universal message server of FIG. 1, including an access restriction filter.

FIG. 3 is a flow diagram of a method of processing electronic messages.

FIG. 4 is a flow diagram of a method of interrogating an electronic message for an access restriction notice.

FIG. 5 is a flow diagram of a method of responding to a detected access restriction notice in accordance with a prescribed transmission policy.

DETAILED DESCRIPTION

Referring to FIG. 1, in one embodiment, a universal messaging system 10 (e.g., an Xpressions™ universal messaging system, available from Siemens Information and Communication Networks of Boca Raton, Florida, U.S.A.) includes a universal message server 12 (e.g., an Exchange server available from Microsoft Corporation of Redmond, Washington, U.S.A.) that is coupled to a local area network (LAN) 14. A communications server 16 couples communications terminals, including a fax machine 18 and a telephone 20, to LAN 14. In addition, one or more personal computers (or workstations) 22 may be coupled to LAN 14. LAN 14 is coupled to an external network 24 (e.g., the Internet) to enable users to exchange messages with people who are not directly connected to the local area network. Universal message server 12 handles the receipt and transmission of electronic messages from a variety of different message sources 26, including e-mail messages 28, voice mail messages 30, fax messages 32 and video messages 34. Universal message server 12 provides a single repository for e-mail messages 28, voice mail messages 30, fax messages 32 and video messages 34. In operation, universal messaging system 10 provides unified messaging services for handling voice mail, fax, e-mail and other media types. In particular, universal messaging system 10 provides an all-in-one mailbox or personal message center that users may access to manage their electronic messages using a personal computer or a telephone (and in some embodiments using a personal digital assistant (PDA) or an Internet-enabled digital phone).

As shown in FIG. 2 and explained in detail below, universal message server 12 includes an access restriction filter 40 that is configurable to prevent intentional and

unintentional transmission of electronic messages subject to one or more access restriction conditions. In this way, access restriction filter can protect users and their employers from potential liability (e.g., liability to copyright owners for unauthorized reproduction or distribution of their copyrighted works) and potential loss of corporate assets (e.g., trade secret information) that otherwise could result from the intentional or unintentional distribution of certain kinds of electronic messages.

Referring to FIGS. 2 and 3, in one embodiment, access restriction filter 40 includes a message interrogator 42 that is configured to interrogate or check an electronic message for an access restriction notice. Access restriction filter 40 also includes one or more prescribed transmission policies 44 specifying the way in which access restriction filter 40 responds to detected access restriction notices. As shown in FIG. 3, in one embodiment, access restriction filter 40 is configured to process an electronic message as follows. In response to a user command to transmit an electronic message (step 50), access restriction filter 40 interrogates the electronic message for an access restriction notice (step 52). If an access restriction notice is not detected (step 54), the message is transmitted (step 56); otherwise, access restriction filter 40 responds in accordance with one or more of the prescribed transmission policies 44 (step 58).

As used herein, the term "electronic message" refers broadly to an encapsulation of one or more data objects each of which may include any type of electronic content, including text, graphics, data, digitized voice and image content. An electronic message may include a primary message and any number of attachments. In addition, the term "access restriction notice" is intended to refer to any notice restricting access to information associated with the notice. Exemplary access restriction notices include "Copyright," "Confidential," "Attorney-Client Privileged" or "Attorney Work Product," "Proprietary" and "Internal Use Only."

Referring to FIG. 4, in one embodiment, the way in which access restriction filter 40 interrogates an electronic message depends on the type of content contained in the message. If the electronic message contains computer-readable characters (e.g., text represented by ASCII codes) (step 60), characters in the message are compared to one or more stored access restriction notices (step 62). For example, if the electronic message contains an e-mail message or a text document, access restriction filter 40 may search the entire e-mail message or text document for a copyright notice symbol (©). Alternatively, access restriction filter 40 may search the entire e-mail message or text document for

certain kinds of access restriction notices (e.g., "Confidential," "Proprietary" and "Internal Use Only"). With respect to certain multimedia files that include text headers, such as audio files (e.g., MP3 files and WAV files), access restriction filter 40 may search the header for any access restriction notice. If an access restriction notice is detected (step 64), access restriction filter 40 responds in accordance with one or more prescribed message transmission policies (step 66). If the electronic message contains a still image (e.g., a TIF, XIF, BMP, JPEG, GIF or PDF image) (step 68), access restriction filter 40 translates characters in the image into a computer-readable format (e.g., ASCII codes) (step 70). Conventional character recognition technology may be used to translate the image data into computer-readable form. The translated characters are compared to one or more stored access restriction notices (step 72). If an access restriction notice is detected (step 74), access restriction filter 40 responds in accordance with one or more prescribed message transmission policies (step 66). If the electronic message contains video (step 76), access restriction filter 40 compares computer-readable characters in the video header to one or more stored access restriction notices (step 78). If an access restriction notice is detected (step 80), access restriction filter 40 responds in accordance with one or more prescribed message transmission policies (step 66). Otherwise, access restriction filter 40 translates characters in each video frame into a computer-readable format (e.g., ASCII codes) (step 82), and compares the translated characters to one or more stored access restriction notices. If an access restriction notice is detected (step 86), access restriction filter 40 responds in accordance with one or more prescribed message transmission policies (step 66). Otherwise, the message is transmitted (step 88).

As shown in FIG. 5, in one embodiment, access restriction filter may respond to a detected access restriction notice in a variety of ways. For example, in some embodiments, if an access restriction notice is detected (step 100) and a user override option is enabled (step 102), the user may override the access restriction (step 104). If a user override is not received (step 104), access restriction filter 40 blocks the transmission of the message (step 106) and reports to the user that the transmission was blocked because an access restriction notice was detected in the message (step 108). In some embodiments, an electronic message may be sent to a system administrator who would approve or deny a user's request to override a block message transmission (for "Attorney-Client Privileged" or "Attorney Work Product," an electronic message might be sent to the legal department for approval or denial of a user's request to override a block message transmission). In some embodiments, even if the user override option is not enabled (step

102), the user may be allowed to transmit a message containing an access restriction notice if a fee payment option is available (step 110). For example, certain copyrighted works (e.g., works registered with the National Copyright Clearinghouse) contain notices indicating that users may make reproductions of the works for a prescribed fee. If the fee payment option is available (step 110), access restriction filter 40 detects the required fee identified in the electronic message and displays the required fee to the user (step 112). If the transmission fee is collected (step 114), the message may be transmitted (step 116). Otherwise, access restriction filter 40 blocks the transmission of the message (step 106) and reports to the user that the transmission was blocked because the required transmission fee was not paid (step 108).

The systems and methods described herein are not limited to any particular hardware or software configuration, but rather they may be implemented in any computing or processing environment. Access restriction filter 40 preferably is implemented in a high level procedural or object oriented programming language; however, the program may be implemented in assembly or machine language, if desired. In any case, the programming language may be a compiled or interpreted language.

Other embodiments are within the scope of the claims. For example, the way in which access restriction filter 40 responds to a detected access restriction notice may vary depending upon the nature of the access restriction. Electronic messages containing copyrighted works may be blocked unless a fee payment option is available and the required fee is collected, as described above. Electronic messages containing limitations on the number or kinds of people who may receive the messages (e.g., proprietary works, confidential works and for internal use only works) may be blocked or they may be transmitted to only certain persons or certain classes of persons (e.g., persons within the same company). The names of the authorized recipients or the classes of authorized recipients may be identified in an electronic message subject to an access restriction condition, or access restriction filter 40 may be configured to respond to such notices in a predetermined way (e.g., transmission policies 44 may identify the names or classes of authorized recipients).